Technická univerzita v Liberci

FAKULTA PŘÍRODOVĚDNĚ-HUMANITNÍ A PEDAGOGICKÁ

Katedra: Katedra tělesné výchovy

Studijní program: B6208 Ekonomika a management

Studijní obor: Management sportovní

PROBLÉMY VNÍMÁNÍ BEZPEČNOSTI INFORMACÍ

PROBLEMS OF PERCEPTION OF INFORMATION SECURITY

Bakalářská práce: *11*–FP–*KTV*– 408

Autor:

Andrea Kulhánková

Podpis:

.....

Vedoucí práce: Ing. Zbyněk Hubínka

Počet

stran	grafů	obrázků	tabulek	pramenů	příloh
56	18	3	3	23	3

V Liberci dne: 26. 4. 2011

Čestné prohlášení

Název práce: Problémy vnímání bezpečnosti informací

Jméno a příjmení autora: Andrea Kulhánková

Osobní číslo: P08000557

Byl/a jsem seznámen/a s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo.

Prohlašuji, že má bakalářská práce je ve smyslu autorského zákona výhradně mým autorským dílem.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval/a samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Prohlašuji, že jsem do informačního systému STAG vložil/a elektronickou verzi mé bakalářské práce, která je identická s tištěnou verzí předkládanou k obhajobě a uvedl/a jsem všechny systémem požadované informace pravdivě.

V Liberci dne: 26. 04. 2011

.....

Andrea Kulhánková

Poděkování

Ráda bych zde vyjádřila poděkování vedoucímu mé bakalářské práce Ing. Zbyňku Hubínkovi za cenné rady, které mi poskytl při vedení práce, za ochotu a trpělivost. Dále bych ráda poděkovala všem respondentům, kteří zodpověděli můj dotazník. Děkuji také dalším lidem, především rodině, kteří mi byli při psaní bakalářské práce velikou oporou.

PROBLÉMY VNÍMÁNÍ BEZPEČNOSTI INFORMACÍ

Anotace:

Bakalářská práce na téma „Problémy vnímání bezpečnosti informací“ je zaměřena na problematiku počítačové bezpečnosti a jejím hlavním cílem je na základě analýzy současné situace a obecného povědomí podat přehled možností ochrany informací před zneužitím osobami, skupinami nebo organizacemi, jejichž primární činnost je zaměřena právě na získávání a vytěžování důvěrných informací.

Teoretická část bakalářské práce je věnována seznámení s vybranými pojmy, které mohou ovlivnit problematiku počítačové bezpečnosti. V praktické části byl proveden rozbor výsledků dotazníku, který byl vytvořen a distribuován pro potřeby této bakalářské práce. Úkolem dotazníku bylo zjistit aktuální situaci v povědomí uživatelů počítačů vzhledem k zabezpečení počítače.

Z výsledků vyplývá, že malá míra informovanosti uživatelů počítačů přímo ovlivňuje nedostatečnou úroveň zabezpečení jejich počítačů. Tyto poznatky by bylo možné aplikovat v praxi a dosáhnout tak zvýšení míry informovanosti populace v dané problematice.

Klíčová slova:

Osobní počítač, počítačová bezpečnost, antivirový program, malware, hacker.

PROBLEMS OF PERCEPTION OF INFORMATION SECURITY

Annotation:

The bachelor thesis, that is entitled „Problems of Perception of Information Security“, is focused on the problems of computer security and the main aim of the bachelor thesis is to show an overview of the possibilities of protecting information from abuse by people, groups or organizations whose primary activity is currently focused on acquiring and exploitation of confidential information based on an analysis of current situation and general awareness.

The theoretical part is devoted to acquaintance with selected terms that can affect computer security issue. A study of the questionnaire results which was created and distributed for the purposes of this thesis was performed in the practical part. The task of the questionnaire was to establish a current situation in the computer users' awareness in the view of computer protection.

The results show that poor computer users' awareness directly influences the insufficient level of their computer protection. These findings could be applied in practice to achieve increase in the population awareness in this area.

Key words:

Personal computer, computer security, antivirus program, malware, computer hacker.

OBSAH

ÚVOD 10
1 CÍLE PRÁCE 11
1.1 Hlavní cíl 11
1.2 Dílčí cíle 11
2 PROBLEMATIKA POČÍTAČOVÉ BEZPEČNOSTI 12
2.1 Pohled do historie 14
2.1.1 Vznik a vývoj malware 15
2.1.2 Současné trendy 15
2.2 Druhy malware 16
2.2.1 Počítačové viry 17
2.2.2 Trojské koně 19
2.2.3 Červi 20
2.2.4 Backdoor 20
2.2.5 Spyware 21
2.2.6 Adware 22
2.2.7 Phishing 22
2.2.8 Dialer 24
2.2.9 Rootkit 24
2.3 Speciální druhy infiltrace 25
2.3.1 Spam 25
2.3.2 Hoax 25
3 JAK CHRÁNIT SVŮJ POČÍTAČ? 27
3.1 Antivirová ochrana počítače 27
3.1.1 Antivirové systémy 28
3.1.2 Firewall 29
3.1.3 Antispam 30
3.1.4 Antispyware 30
3.1.5 Antibanner, antipopup a podobné 31
3.2 Ochrana dat před selháním techniky 31
3.3 Ochrana dat před dalšími vlivy 33

3.3.2 Endogenní vlivy ... 33
3.3.1 Exogenní vlivy ... 33
4 KDYŽ JE POČÍTAČ INFIKOVÁN ... 35
4.1 Vlastní pomoc ... 35
4.2 Odborník ... 35
5 DOTAZNÍK PREFERENCE UŽIVATELŮ V OBLASTI ZABEZPEČENÍ POČÍTAČE ... 39
5.1 Obsah dotazníku ... 39
5.2 Vyhodnocení dotazníku ... 39
5.2.1 Technické vybavení respondenta ... 39
.2.2 Stav ochrany PC ... 40
5.2.3 Orientace respondenta v terminologii ... 46
5.2.4 Zkušenosti respondenta ... 47
5.3 Shrnutí dotazníku ... 50
ZÁVĚR ... 52
SEZNAM POUŽITÉ LITERATURY ... 54
PŘÍLOHY ... 56

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

FTP	- File Transfer Protocol, protokol na síti internet určený pro přenos souborů
HTTP	- Hypertext Transfer Protocol, hypertextový přenosový protokol
HTTPS	- Hypertext Transfer Protocol Secure, zabezpečená verze protokolu HTTP
IT	- Information Technology, informační technologie
LAN	- Local Area Network, místní počítačová síť
MS	- Microsoft
OS	- Operating System, operační systém
PC	- Personal Computer, osobní počítač
RAID	- Redundant Array of Independent Disks, vícenásobné diskové pole nezávislých disků
SSH	- Secure Shell, zabezpečený komunikační protokol v počítačových sítích
SSL	- Secure Socket Layer, vrstva bezpečných socketů zabezpečujících autentizaci a šifrování komunikace
TCP, UDP	- Transmission Control Protocol, User Datagram Protocol, protokoly umožňující komunikaci počítačů v internetu
UPS	- Uninterruptible Power Supply, nepřerušitelný zdroj napájení
USB	- Universal Serial Bus, univerzální sériová sběrnice
VGA	- Video Graphics Array, počítačový standard pro počítačovou zobrazovací techniku
VPN	- Virtual Private Network, virtuální privátní síť

ÚVOD

K výběru tématu pro bakalářskou práci mě motivovala zejména osobní zkušenost a zároveň snaha věnovat se ve své bakalářské práci problematice, která se týká široké veřejnosti. Troufám si tvrdit, že téma počítačové bezpečnosti je zvláště v dnešní době (v době, kdy osobní počítač nebo notebook a s nimi i internetové připojení je naprostou samozřejmostí) velice aktuální. Také jsem chtěla vytvořit práci, která by do budoucna mohla pomoci potenciálním zájemcům zorientovat se v tak rozsáhlém oboru, jakým počítačová bezpečnost je. Aktuálnost tématu a možnost přiblížit problémy vnímání bezpečnosti informací širší veřejnosti by měly charakterizovat mou práci.

Nejen pro mě je otázka bezpečnosti informací zásadní, je nutné si uvědomit, že aby se předešlo nechtěné ztrátě informací a dat, nesmí se jejich ochrana podcenit. Mnohdy jsou informace velice cenné, cennější než hmotný majetek, a právě proto je dnes na jejich ochranu kladen velký důraz.

Bakalářská práce je rozvržena do pěti kapitol. První kapitola se bude věnovat vymezení konkrétních cílů této bakalářské práce. Druhá a třetí kapitola jsou teoretického rázu a jejich úkolem je seznámení s danou problematikou. Pozornost bude věnována především stručnému popisu vývoje počítačové infiltrace, vymezení pojmů souvisejících s tématem a popisu jednotlivých částí antivirové ochrany.

Ve čtvrté kapitole budou diferencovány názorně případy opravy poruchy výpočetní techniky běžným uživatelem a odborníkem. Obsahem páté kapitoly bude vyhodnocení dotazníku, který byl zaměřen převážně na tzv. „domácí uživatele“ a jehož cílem bylo zjistit úroveň povědomí v problematice počítačové bezpečnosti.

Ke zpracování a analýze nasbíraných dat byly použity statistické metody a výsledky jsou v práci prezentovány v podobě tabulek a grafů.

1 CÍLE PRÁCE

1.1 Hlavní cíl

Cílem bakalářské práce je na základě analýzy současné situace a obecného povědomí podat přehled možností ochrany informací před zneužitím osobami, skupinami nebo organizacemi, jejichž primární činnost je zaměřena právě na získávání a vytěžování důvěrných informací.

1.2 Dílčí cíle

1. Teoretické seznámení s danou problematikou.
2. Přehled možností ochrany počítače před ztrátou informací.
3. Vytvoření dotazníku a jeho distribuce respondentům.
4. Analýza nasbíraných dat.
5. Zhodnocení současné situace a doporučení pro nápravu.

2 PROBLEMATIKA POČÍTAČOVÉ BEZPEČNOSTI

Důležitou a velmi choulostivou stránkou zabezpečení dat je jejich ochrana před zneužitím nepovolanými osobami a skupinami či dokonce organizacemi, jejichž primární činnost je zaměřena právě na získávání důvěrných informací a jejich následné zpeněžení.

Povinnost ochrany spravovaných dat před zneužitím je v mnoha případech dokonce upravena zákonem, bohužel mnohdy pouze formálně a v hrubých rysech. Samotné pojmy „*důvěrná data*“ a „*zneužití*“ jsou stejně jako mnoho dalších právnických termínů nepřesně terminologicky vymezené. V současné době lidé už téměř přivykli každodenním telefonním nabídkám různých výhodných úvěrů a půjček, dovolených a jiných. Většina těchto „obchodních nabídek“ nemusí být v souladu s platnými právními předpisy a může jim předcházet kriminální delikt z oblasti zneužití důvěrných dat.

Jiné a mnohem citlivěji vnímané je obvykle zneužití osobních dat při platebním styku nebo například ve zdravotnictví. Podobných příkladů zneužití důvěrných dat je nepřeberné množství, nejcitlivěji jsou postiženy následující oblasti:

- **komunikační operátoři** – únik osobních dat, adres, tel. čísel apod.,
- **veřejná správa** – únik osobních dat, zneužití územních plánů apod.,
- **finanční ústavy** – únik osobních dat, zabezpečovacích prvků,
- **firmy** – únik průmyslového tajemství,
- **armáda** – únik vojenského tajemství,
- **sdělovací prostředky** – zneužití a nelegální získávání informací,
- a jiné oblasti, kde lze zneužitá data výhodně zpeněžit.

Zneužití dat lze přitom ve většině případů s minimálními investicemi předejít, případně alespoň výrazně snížit pravděpodobnost jeho výskytu. Mezi nejběžnější ochranné principy patří zejména:

- neposkytování údajů neoprávněným osobám,
- poskytování jen nezbytného minima údajů,
- používání zabezpečovacích prvků, např. „*silných hesel*“ apod.,
- využívání a vyžadování přístupových a kvalifikačních certifikátů a certifikačních autorit,
- využívání zabezpečených transportních protokolů a šifrovaných komunikačních kanálů (SSL, SSH, HTTPS…) pro přenos dat,
- využívání virtuálních privátních sítí (VPN) pro vzdálenou komunikaci s firemními sítěmi,
- používání vhodného firewallu na obou koncích komunikačního kanálu,
- používání komplexně propracovaného antivirového systému,
- pravidelné aktualizace operačního systému, aplikací a především antiviru,
- uživatelská kázeň při používání internetu,
- obezřetnost při otevírání e-mailů (zejména z neprověřených zdrojů),
- oddělení vážné práce od zábavy (nejlépe vyčleněním jiného PC),
- profylaxe - pravidelné návštěvy odborníka.

Nejběžnější námitkou uživatele PC obvykle bývá, že kvalitní zabezpečení dat je finančně náročné. Pořízení Windows, Office, antivirového systému s firewallem, certifikátů a podobných nezbytností vyžaduje investování nemalých finančních částek. Ve srovnání s potenciální škodou a nutnými následnými výdaji na opravu bývá však tato investice často nepatrným zlomkem, navíc moudře vynaloženým.

Všeobecně rozšířeným omylem, nicméně mezi uživateli velmi populárním, je domněnka, že za vznikem a masívním šířením virů stojí firmy produkující antivirové programy. Ptáme-li se „Komu ku prospěchu“, pak reálnějšími viníky jsou:

- hackeři či skupiny hackerů snažící se o proniknutí do vašeho PC za účelem získání důvěrných informací, dokumentů, přístupových hesel, seznamů kontaktů apod. Většinou za tímto počínáním stojí snaha jejich dalšího prodeje, přirozeně nelegálního, ale o to více honorovaného.
- podobné skupiny, které se snaží informace využít bezprostředně, například zneužitím platebních karet, přístupu k firemnímu účtu apod.
- firmy rozesílající nevyžádanou reklamu. Mnohdy ale pod zástěrkou reklamy číhá léčka vedoucí k výše uvedeným aktivitám.
- oficiální špionážní služby s politickým, vojenským či hospodářským kontextem. Jde obvykle o nejlepší profesionály svého oboru.
- odborníci v dané oblasti rozhodnuti poškodit např. bývalého zaměstnavatele, kolegu, konkurenci apod.
- nezanedbatelné procento počítačových nadšenců, experimentátorů a dalších.

2.1 Pohled do historie

Vznik a vývoj prvních virů v nejširším slova smyslu je poměrně přesně zmapovaný a možno říct, že v mnoha případech nemusel nutně být doprovázen zlým úmyslem. Často šlo prostě o experimenty, které se autorům vymkly z kontroly nebo byly následně zneužity.

2.1.1 Vznik a vývoj malware

Počátkem 70. let minulého století se začínají objevovat první případy počítačové infiltrace. Historie počítačové infiltrace je velmi zajímavá, ale také velmi obsáhlá a není předmětem této práce, proto je zde vymezen pouze výčet několika virů, které nějakým způsobem významně ovlivnily vývoj zákeřného softwaru:

- **Pervading Animal (1975)** - počítačový virus, který formou epidemie škodil na systémech Univac 1108.
- **The Creeper** - program šířící se globální počítačovou sítí. Na boj proti tomuto viru byla vytvořena první obdoba antivirového programu – program Reeper.
- **Elk Cloner (1982)** – autorem virusu, který napadal a infikoval stroje Apple II, byl patnáctiletý mladík Richard Skrenta z Pensylvanie.
- Studie **Computer Viruses - Theory and Experiments (1984) -** dílo amerického studenta Freda Cohena.
- **Brain (1986)** - šířil se přes diskety. Brain byl prvním virem určeným pro počítače, tedy pro operační systém MS-DOS.
- **Jerusalem (1988)** – cílem viru bylo původně několik společností a univerzit, ale infikoval nespočet počítačů po celém světě. Vyvolal doslova pandemii, především „díky“ tomu, že antivirové programy ještě nebyly běžnou záležitostí. [12]

2.1.2 Současné trendy

Podoba a mechanismus činnosti virů v PC se vyvíjely podle charakteristik doby a prostředí, ve kterém existovaly. Vývoj těchto virů byl závislý na jejich možnosti přizpůsobit se novým podmínkám. Každý případ infiltrace je postupem času objeven, zmapován a odchycen. Naprostá většina virů dnes využívá k šíření, duplikaci a jiné své činnosti nového informačního média - internetu. Přirozeně přitom postupují cestou nejmenšího odporu, čili napadají především méně zabezpečené internetové servery. Těmi už tradičně jsou pornoservery a servery

s nelegálním software, filmy a hudbou. Odtud je ideální cesta k miliónům dalších klientských PC a následnému nekontrolovanému šíření. Jedinou návštěvou takovýchto internetových serverů může být PC uživatele zaplaveno počítačovou infekcí a stát se jejím dalším nechtěným šiřitelem, v horším případě i prostředkem kriminálního deliktu.

Zajímavá je z hlediska vývoje virů také změna chování viru k hostitelskému PC. Dřívější princip „napadnout a co nejdříve vyřadit“ byl nyní nahrazen principem „napadnout a co nejdéle nechat žít“, aby mohlo dojít k nejefektivnější primární (množení) i sekundární (skutečný zlý úmysl) činnosti viru.

V současné době jsou „čistokrevné viry“ na ústupu, resp. jsou nahrazovány efektivnějšími variantami infiltrace, všeobecně nazývané malware.

2.2 Druhy malware

Výraz malware, neboli složení dvou anglických slov „malicious“ (zákeřný) a „software“, se ustálil jako označení pro všechny programy existující v kybernetickém světě, jejichž výskyt v počítači je nežádoucí. Malware je všeobecně velice široký pojem a jeho další rozdělení je složité už z toho důvodu, že se jednotlivé programy vzájemně prolínají a průběžně vyvíjejí. Členění v této práci přirozeně reprezentuje současnou dobu a její komunikační prostředky. Vývoj informačních technologií zákonitě povede k dalším a dalším kategoriím škodlivého software, pokud nedojde k významným změnám v oblasti primárního zabezpečení operačních systémů. [22]

Nástin základního dělení malware naznačuje obrázek č. 1.

Obrázek č. 1 Základní rozdělení malware

Zdroj: <www.svethardware.cz>

2.2.1 Počítačové viry

Počítačový virus je velmi podobný svému biologickému protějšku, také se připojí k nic netušícímu nositeli. Oba termíny mají ještě jednu společnou vlastnost, a to schopnost množení sebe sama. Hostitelem počítačového viru často bývají systémové soubory nebo oblasti disku, popř. různé aplikace, jako např. word nebo excel. Počítačový virus je tedy škodlivý, ale nijak složitý, program, který se po spuštění snaží rozmnožit do ostatních souborů. [9]

V oblasti vzniku a vývoje počítačových virů má nesmazatelné zásluhy američan Fred Cohen. Když ve své studii „*Computer Viruses - Theory and Experiments*“ (v češtině „*Počítačové viry - teorie a experimenty*“) vůbec jako první použil termín „*virus*“, nikdo ani v nejmenším netušil, že právě položil základy oboru s obratem přes tři miliardy eur. [3]

Viry vyvíjejí v hostitelském PC obvykle autorem předem definovanou primární a sekundární činnost:

- **primární činnost** – duplikace, množení, infiltrace,
- **sekundární činnost**:
  - obtěžující – výpisy nesmyslných hlášení, zaplnění kapacity paměti, komolení dat, obtěžující reklamy, poplašné zprávy apod.,
  - destrukční – zejména napadení dat na disku,
  - špionážní – odeslání či vylákání důvěrných informací,
  - jiné nespecifikované, např. často neúmyslná kolize s jiným software.

Primární činnost je důležitá pouze pro jejich přežití a úspěšné množení. Některé viry, řadící se do skupiny méně nebezpečných, mívají pouze tuto primární činnost. Obvykle jsou jen jakýmsi průzkumníkem vyslaným pro ověření schopností nově modifikovaného viru.

Skutečně nebezpečná je až sekundární činnost viru. Zde pak platí: čím nenápadnější jsou projevy viru, tím větší škodu stihne virus napáchat, než uživatel pojme podezření, provede antivirovou kontrolu a virus odhalí a zneškodní.

Viry v zásadě využívají bezpečnostních děr v operačních systémech a aplikacích, nedostatečného zabezpečení komunikačních kanálů a liknavosti uživatelů PC v přístupu k antivirové ochraně. Pokud jsou tyto faktory umocněny nedostatečnou (nebo žádnou) péčí o data v PC, hrozí uživateli PC nebo příslušné firmě reálné škody, schopné ohrozit jejich peněženku či chod firmy.

V případech větších organizací a ve speciálních případech (armáda, zdravotnictví, burza apod.) může případná škoda dokonce ohrozit i lidské životy nebo výrazně oslabit stabilitu státu.

Podle způsobu napadení a typu hostitele lze viry rozdělovat do dalších skupin.

Viry podle umístění v paměti:

- rezidentní,
- nerezidentní. [13]

Dělení virů podle oblastí, které jsou napadeny:

- boot viry,
- souborové viry,
- makroviry,
- adresářové (clusterové) viry,
- generické viry,
- skriptové viry. [13]

Druhy virů podle chování:

- stealth a substealth (utajené a poloutajené) viry,
- polymorfní viry,
- obrněné (schopné sebezakódování),
- retroviry (odvetné). [13]

2.2.2 Trojské koně

Již sám název „Trojský kůň“ napovídá, že se jedná o zdánlivě užitečný program, který představuje skrytou hrozbu pro počítač. Antivirové programy pouze lokalizují trojského koně. Program, který je nakažen trojským koněm, může poškodit počítač a jedinou možností, jak počítač vyčistit, je smazání souboru s trojským koněm. Tento škodlivý kód není, na rozdíl od červů a virů, schopen sebe-replikace.

Trojských koní rozlišujeme dnes hned několik forem, jako jsou například Password-stealing trojani, destruktivní trojani, Trojan Downloader či Trojan Proxy a jiné. Každý z těchto trojských koní se zaměřuje na specifickou formu útoku. Například Password-stealing trojani mají například za úkol, jak už název napovídá, zjistit a přeposlat na cizí emailovou adresu uživatelovy přihlašovací údaje k nejrůznějším službám.

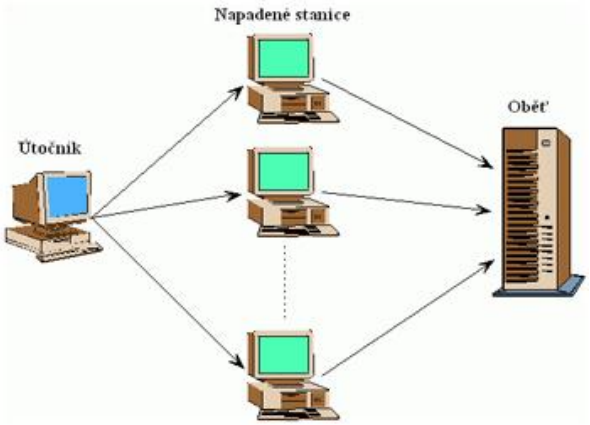
2.2.3 Červi

Jak uvádí výkladový slovník: *„Červ je škodlivý kód, který pro své šíření využívá jakékoliv sítě (lokální i globální). Červ je, na rozdíl od viru, schopen běžet nezávisle na uživateli a šířit se po síti.“* [22]

Červi využívají bezpečnostních děr operačních systémů nebo jiných aplikací, vůbec nejčastěji se šíří prostřednictvím emailů.

2.2.4 Backdoor

Backdoor můžeme z angličtiny přeložit jako „zadní vrátka“. Díky tomuto kódu se dokáže útočník dostat do systému bez ověření totožnosti a bez vědomí uživatele. Na obrázku č. 2 vidíme, že útok na napadenou stanici probíhá skrze prostředníka.



Obrázek č. 2 Schéma útoku přes prostředníka

Zdroj: <www.svethardware.cz>

Rozdělení backdooru dle Krále: „*Backdoory lze rozdělit na dvě části: klientskou a serverovou. Serverová část backdooru se usadí v počítači postiženého uživatele a pomocí klientské části, kterou vlastní útočník, lze serverovou část, a tak zároveň počítač postiženého uživatele na dálku ovládat*.“ [13] Takto zmanipulovaný počítač se pak snadno stává prvkem botnet – sítě počítačů, které pracují pro útočníka.

Zadní vrátka nemusí být vždy jen škodlivým kódem, lze je využít i jako tzv. vědomou bezpečnostní díru.

2.2.5 Spyware

Spyware je speciálním druhem infiltrace, který dokáže využít internetové připojení k tomu, aby nepozorovaně odeslal data z počítače napadeného a nic netušícího uživatele. Tato data mívají statistický charakter, mohou to být například údaje o navštívených stránkách, nainstalovaných programech či třeba seznamy jmen a dokumenty uložené v uživatelově počítači. Program může být mimo jiné šířen společně s řadou různých sharewarových programů. Tento druh špionáže nepatří mezi nejnebezpečnější formy útoku (v horším případě „pouze“ zhoršuje funkci počítače) a je dokonce sporné označit jej paušálně za ilegální. Útočníky je dokonce často šíření spyware označováno jako cesta ke zjištění zájmů a potřeb uživatele, získané informace prý pomohou při dalším vývoji aplikací.

2.2.6 Adware

Název pro Adware vznikl z anglických slov advertising supported software, v češtině něco jako software s reklamou. Většinu z nás tato reklama v podobě vyskakujících pop-up oken (k vidění na obrázku č. 3), reklamních proužků (bannerů) a jiných obtěžuje. Nutno ale dodat, že programy obsahující tuto formu reklamy mají zpravidla bezplatnou licenci. Díky licenčnímu ujednání EULA (z anglického End User License Agreement) by zpravidla měl mít uživatel možnost nesouhlasit s instalací tohoto druhu malware. Na rozdíl od spyware zde nedochází k nevědomému odesílání dat z počítače.

Obrázek č. 3 Typická podoba vyskakujících popup oken

Zdroj: <www.svethardware.cz>

2.2.7 Phishing

Phishing je označován jako podvodné emailové sdělení, které se snaží z uživatele vylákat informace (typicky se jedná o přístupové údaje k účtům - číslo účtu, pin, heslo do internetového bankovnictví atp.). Tyto informace pak využije podvodník ve svůj prospěch.

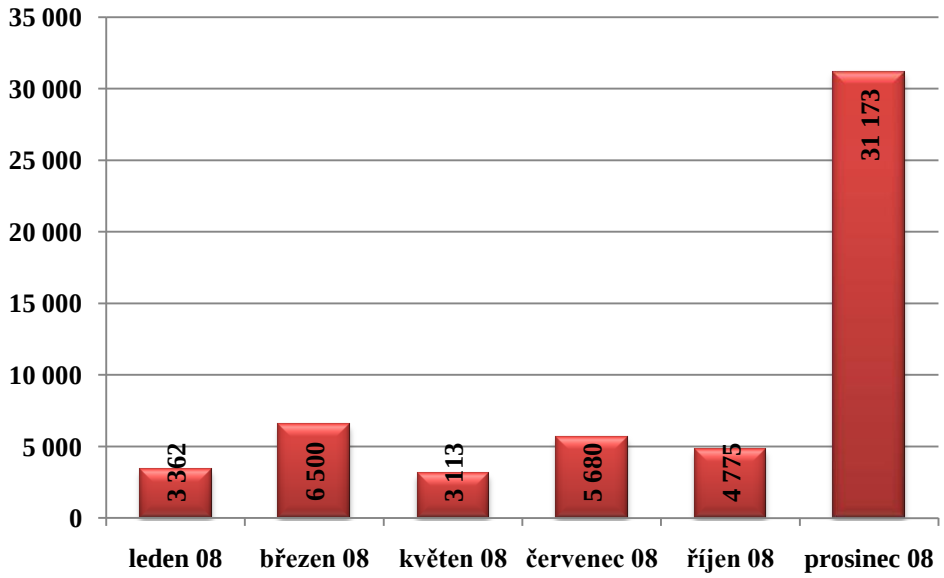
Email má působit jako důležité sdělení od banky nebo spořitelny, kde má uživatel založen účet, a snaží se uživatele přesvědčit, aby kliknul na odkaz, přes

který se dostane na jejich oficiální stránky (realita je taková, že se uživatel octne na podvržených stránkách, které se jen tváří jako oficiální). Pokud neopatrný uživatel v této chvíli vyplní některé ze svých údajů, mají podvodníci vyhráno. Důležité je brát na vědomí, že banka v žádném případě nemá důvod požadovat po vás důvěrné informace prostřednictvím emailu s odkazem.

S pojmem phishing úzce souvisí také pojem sociální inženýrství. Sociální inženýrství se dá charakterizovat jako metoda (podvodného) získávání informací od uživatelů počítače, aniž by o tom měli uživatelé tušení. Je to tedy metoda založená na lidské naivitě, nezkušenosti a hlouposti.

Phishingové emaily jsou rozesílány na velké množství adres a z této jejich vlastnosti také vychází anglický název „phishing“ - výměnou „f“ za „ph“ dostaneme slůvko fishing - rybaření. Podvodníci totiž rozešlou email mnoha náhodně vybraným příjemcům a čekají, kdo této zprávě uvěří a poskytne důvěrné informace.

Jak vyplývá z grafu č. 1, v roce 2008 stoupl celosvětově počet podvržených stránek více o 927 %. [3]



Graf č. 1 Počet podvržených stránek v roce 2008

Zdroj: <http://earchiv.chip.cz/cs/earchiv/vydani/r-2009/chip-07-2009/prulom-silou-grafiky.html>

V české republice není phishing neznámým pojmem, první prokázaný útok se u nás objevil již v březnu 2006. Ovšem zatím největší útoky byly zaznamenány na klienty České spořitelny v roce 2008. První pokusy se prozradily nedokonalou češtinou. Avšak i problém s nedokonalostí strojového překladu dokázali brzy podvodníci překonat a svou trpělivostí se zasíláním podvodných emailů znepříjemňovali život mnoha lidem po dobu několika měsíců.

Hlavními body v obraně proti phishingu je zachování základních pravidel chování na internetu. Je doporučeno ignorovat jakékoliv odkazy v emailové zprávě a přihlašovat se ke svým emailovým, bankovním a jiným účtům vždy ze svého počítače, který je chráněn aktualizovaným antivirovým programem. [7]

2.2.8 Dialer

Jedná se o program, který bez vědomí uživatele dokáže pozměnit telefonické připojení sítě. Tedy místo klasického telefonního čísla vašeho poskytovatele dialer přesměruje linku na hovor s dražší tarifikací. Běžný uživatel tuto skutečnost nezjistí a surfuje po internetu, překvapení potom přijde společně s fakturou. Ochranou proti dialerům je pravidelně aktualizovaný operační systém, kvalitní firewall a antivirový program, ale také používání tzv. antidialeru, tedy programu, který zabrání přesměrování telefonního čísla. Uživatel se může také chránit tak, že si u svého operátora nechá zablokovat hovory do zahraničí a hovory na tzv. žluté linky. Nebezpečí dialerů je naštěstí dnes už téměř minulostí, stejně jako přístup na internet prostřednictvím vytáčeného připojení.

2.2.9 Rootkit

Dříve byl pojem rootkit spojován pouze s operačním systémem UNIX, dnes už je také „záležitostí“ operačního systému Microsoft Windows. Funkcí rootkitu je skrýt a zamaskovat činnost útočníka, vlastní přítomnost v počítači, popřípadě existenci jiných aplikací (programů). Na pomoc proti rootkitu se doporučují programy speciálního charakteru, protože běžný antivirový program počítač nedokáže ochránit se stoprocentní jistotou. [22]

2.3 Speciální druhy infiltrace

Vedle malware jsou významným nešvarem dnešního počítačového světa spamy (nevyžádané zprávy), hoaxy (poplašné zprávy) a podobná nesoftwarová infiltrace. Její detekce bývá mnohem obtížnější a vyžaduje obvykle aktivní zapojení uživatele PC.

2.3.1 Spam

Spamem se rozumí obtěžující nevyžádaná pošta, často je také označován jako reklamní balast či odpad. Spam má často reklamní charakter a typicky je šířen elektronickou poštou. Spam je v dnešní době celosvětovým fenoménem. Odhaduje se, že podíl nevyžádané pošty v měřítku celosvětové emailové pošty je až 80%. [11]

Jedním ze způsobů, jakým jsou získávány emailové adresy pro šíření spamu, je pomocí vyhledávacích programů, které procházejí internetové stránky a sbírají všechny adresy, které zde naleznou. Nabízí se nám tedy jedna rada, jak se nedostat na takovýto seznam - při poskytování své emailové adresy uvádějte místo symbolu „@“ slovy přepsaný ekvivalent. Emailová adresa uvedená na webové stránce by tedy vypadala např. takto - *andrea.kulhankova“zavináč“tul.cz*. Další možnosti boje proti spamu jsou:

- Sdělujte svou emailovou adresu pouze tomu, od koho chcete, aby vám zprávy přicházely.
- Nikdy neodpovídejte na spam a spamové zprávy neotvírejte. Pokud tak uděláte, jen na sebe upozorníte a dáte najevo, že tato adresa je aktivní. Potom už se spamu nezbavíte. [13]

2.3.2 Hoax

Anglickým termínem hoax je označována poplašná zpráva, jež varuje před neexistujícím nebezpečím. V České republice, stejně jako po celém světě, je šíření hoaxu prostřednictvím elektronické pošty velice oblíbené. Hromadným přeposíláním emailových zpráv dochází k mystifikaci uživatelů a tento začarovaný kruh se stále rozrůstá a může dosáhnout až obrovských rozměrů globálního charakteru. [6]

Jak uživatel pozná, že se jedná o hoax (aneb co by měl správný hoax obsahovat):

- popis nebezpečí a varování před ním,
- výčet ničivých účinků tohoto nebezpečí,
- upozornění na důvěryhodnost zdrojů informace,
- apel k rozeslání co nejvíce dalším lidem.

Druhy hoaxů (detailní popis k nalezení v databázi hoaxů na internetové stránce hoax.cz):

- varování před smyšlenými viry a různými útoky na počítač,
- popis jiného nereálného nebezpečí,
- falešné prosby o pomoc,
- fámy o mobilních telefonech,
- petice a výzvy,
- pyramidové hry a různé nabídky na snadné výdělky,
- řetězové dopisy štěstí,
- žertovné zprávy a další.

Mnohé možná napadne, že oproti ostatnímu nebezpečí na internetu v dnešní době je hoax sice nepříjemným, ale zcela neškodným nástrojem několika vtipálků. Věc ale není zase tak jednoduchá, vytvářením hoaxu i jeho přeposíláním může dojít i ke značné finanční škodě. Vedle své "obtěžovací" funkce dokáže například poškodit dobré jméno společnosti, proti které je zaměřen. Přeposíláním hoaxů může uživatel na sebe nebo na své známé prozradit důvěrné informace či ztratit důvěryhodnost před svými zákazníky, obchodními partnery i kamarády.

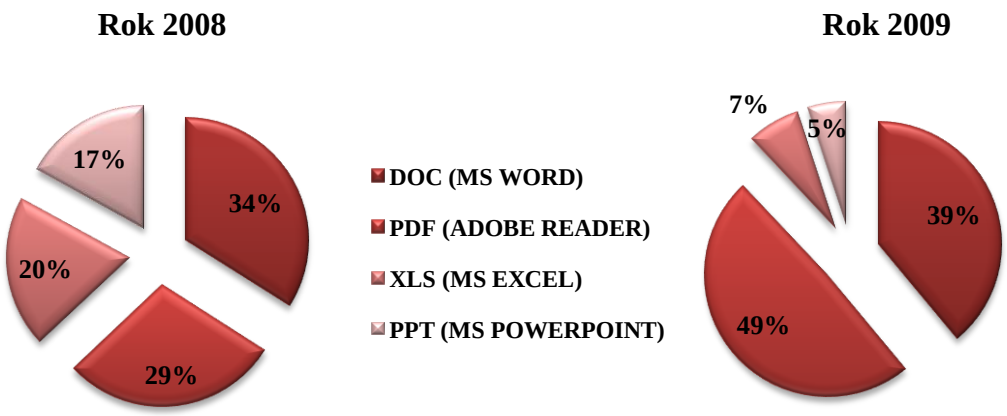
Pokud uživatel obdržel email, o němž ví, že je hoax, neměl by ho v žádném případě přeposílat dál. Jediný způsob, jakým lze reagovat na příchozí hoax, je upozornit na tuto skutečnost taktně odesílatele. [6]

3 JAK CHRÁNIT SVŮJ POČÍTAČ?

3.1 Antivirová ochrana počítače

Při výběru antivirového systému by se měl uživatel vyhýbat polofunkčním verzím typu „*free edition*“. Úspory financí lze lépe dosáhnout cenovým zvýhodněním při koupi antiviru na delší období nebo zakoupením antiviru pro více PC, kdy cena v přepočtu na 1 PC je obvykle výrazně nižší.

V grafu č. 2 můžeme porovnat roční procentuální výskyt útoků na kancelářské dokumenty. Z čísel uvedených v grafu lze vypozorovat, že k šíření virů byly v roce 2008 využívány především soubory z kancelářského balíku MS Office. Naproti tomu v roce 2009 byly ke stejnému účelu největší mírou zneužívány soubory s příponou PDF. [3]



Graf č. 2 Útoky na kancelářské dokumenty

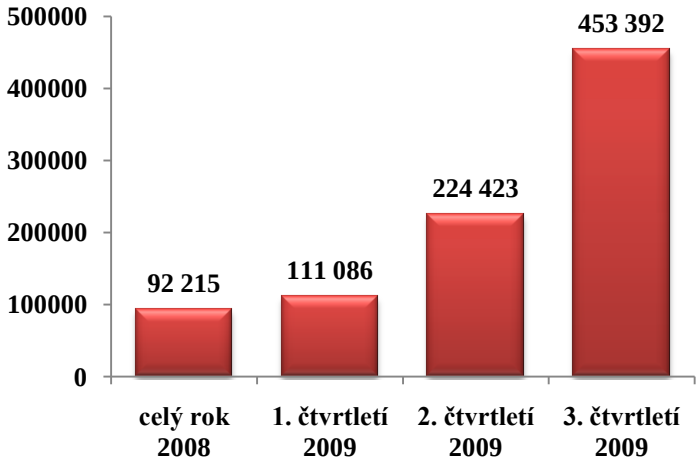
Zdroj: <http://earchiv.chip.cz/cs/earchiv/vydani/r-2009/chip-07-2009/prulom-silou-grafiky.html>

3.1.1 Antivirové systémy

Dobře propracovaný antivirový systém by měl počítač chránit komplexně a měli byste v něm najít následující komponenty:

- **File-antivirus** - kontrola všech otevřených, uložených a aktivních souborů k zajištění neustálé ochrany.
- **Mail-antivirus** - kontrola příchozích a odchozích zpráv na přítomnost nebezpečných objektů.
- **Web-antivirus** - prověřuje informace přijaté prostřednictvím protokolů HTTP a FTP a brání spouštění nebezpečných skriptů v počítači.

Pro seznámení s realitou můžeme nahlédnout do grafu č. 3. Ten nám říká, že v průběhu prvního čtvrtletí roku 2009 bylo odhaleno větší množství falešných antivirových programů než za celý rok 2008. Tyto počty se neustále zvyšují. [3]



Graf č. 3 Trend: falešné antiviry

Zdroj: <http://earchiv.chip.cz/cs/earchiv/vydani/r-2009/chip-07-2009/prulom-silou-grafiky.html>

V příloze č. 3 je k nalezení seznam deseti nejlepších produktů výrobců antivirových systémů sestavený webovým serverem TopList.com.

3.1.2 Firewall

V zásadě je firewall něco jako „bezpečnostní brána“ oddělující provoz mezi dvěma sítěmi (např. naší domácí a internetem), přičemž propouští jedním nebo druhým směrem data podle určitých předem definovaných pravidel. Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele. Technicky jde buď o samostatné zařízení (hmotné, samostatná elektronika + software) či specializovaný software. Softwarový firewall je dnes prakticky povinnou složkou propracovaných antivirových systémů.

Podle nasazení můžeme rozlišovat firewally firemní (pro ochranu celých sítí LAN) a osobní (pro jednotlivé stanice). Lze je navzájem kombinovat, není však doporučeno používat více firewallů v jednom stupni (tj. například pro naše PC), mohlo by dojít k výraznému zpomalení provozu a nežádoucí interferenci firewallů. Firemní firewally jsou obvykle doménou IT specialistů a není tudíž příliš na závadu, pokud vyžadují odborné znalosti (vč. jazykových předpokladů) a pravidelný dozor. Osobní firewall by však měl být přívětivý a všechny funkce nabízet prostřednictvím snadno pochopitelného grafického rozhraní a přirozeně bez předpokladu odborných znalostí.

Jádrem každého firewallu jsou komunikační pravidla. Implicitní bezpečnostní politika, tj. pravidlo č. 1, by se dalo charakterizovat: „co není dovoleno, je zakázáno“. Ostatní komunikační pravidla jsou pak ušitá na míru jednotlivým aplikacím a tvoří tak systém filtrování paketů, informačních balíčků putujících skrze firewall. Většinu komunikačních pravidel má naštěstí firewall ve výbavě od výrobce nebo si je vytvoří při prvotní instalaci. Na samotného uživatele zbude nadefinování komunikačních pravidel popisujících jeho specifické aplikace či prostředí. Nejjednodušší pravidlo pak vypadá asi takto: „Aplikaci X povol TCP i UDP obousměrnou komunikaci na portech 25, 110 a 143, jinak se zeptej uživatele.“ Nebo v případě multifunkční tiskárny: „Povol veškerou komunikaci místní sítě s IP 192.168.1.20.“

Součástí firewallu bývá i správa VPN. V podstatě jde nejčastěji o chráněné propojení místní sítě se vzdálenými PC, která se pak chovají jako součást

zabezpečené místní sítě. Ochrana VPN je zpravidla realizována šifrováním přenosu a použitím bezpečnostního certifikátu.

3.1.3 Antispam

Funkcí antispamu je rozpoznání a označení nevyžádané pošty, jiným slovem spamu, případně i smazání takovéto pošty. I když je téměř stoprocentní jistota, že spam nikdy nevymizí, můžeme ho do určité míry eliminovat.

Tři základní metody rozpoznání spamu:

Bayesovský filtr - analýza spamu probíhá až na základě toho, že uživatel „naučí“ program, která slova má považovat za spam (může se dít i automaticky). Program poté zanalyzuje obsah a vyhodnotí, zda se jedná o spam nebo ne.

Blacklist (černý seznam) - seznam emailových adres, z nichž antispamový program zprávy nepřijímá. Vedle blacklistu existuje také whitelist (bílý seznam - seznam povolených emailových adres).

Testování podle obsahu - založení na vyhledávání slov a slovních spojení, která bývají typickou součástí spamového emailu. Jedná se například o nabídky produktů jako je viagra a jiných zázračných léků, akcií, replik značkových výrobků a mnoho dalších. [13]

Antispamu můžete přispět ke správné detekci, pokud například označíte vámi nevyžádané zprávy jako spam.

Rozdělení antispamu do dvou skupin:

- aplikace určená pro konkrétního e-mailového klienta,
- aplikace univerzální, využitelná pro jakoukoli poštovní aplikaci. [1]

3.1.4 Antispyware

Spyware zpravidla nedokáže odhalit běžný antivirový program. Úkolem programu antispyware tedy je zjistit a odstranit spyware. Pro to, aby mohl vyhledat spyware, je nutná databáze spyware aktualizovaná výrobcem.

Prvním produktem tohoto druhu byl program OptOut p. Steve Gibsona, amerického programátora. V nynější době je antispyware bezplatně ke stažení pro nekomerční uživatele. Pod názvem „Windows Defender“ jej nabízí jako standardní součást pro operační systém Windows společnost Microsoft. [1]

3.1.5 Antibanner, antipopup a podobné

Blokuje ve webovém prohlížeči a v některých aplikacích reklamu a reklamní lišty. Tato reklama je nejen otravující a ztěžuje uživateli práci, ale často právě obsahuje škodlivé kódy.

3.2 Ochrana dat před selháním techniky

Spolehlivost výpočetní techniky se sice neustále zvyšuje, přesto však ani zdaleka nedosahuje celých 100 %. Pravděpodobnost poruchy PC jako souhrnu komponent je pak závislá nejen na součtu pravděpodobností poruch jednotlivých komponent (ovlivnitelných např. pečlivým výběrem dodavatele), ale i na provozních podmínkách (tj. zátěží a péčí o PC), stářím komponentů a působících vnějších vlivech (teplota, prašnost, stálost napětí apod.).

Ve finále počítači uživatele hrozí porucha právě v době, kdy je plný cenných dat. Tou dobou je už lehce opotřebovaný, mírně zanedbaný a uživatelova ostražitost již dávno polevila. Následkem běžné nehody, nepozornosti nebo infikování počítače pak snadno nastane situace, kdy je uživatel bez důležitých dokumentů, obchodní korespondence za několik let, spojení s bankou, internetového připojení, fotografií z dovolené, filmů, hudby atd. Velmi případné pro tyto situace je heslo znějící „*o zálohování dat se stará pouze ten, kdo je aspoň jednou ztratil*“.

Jediná správná a spolehlivá cesta k zabezpečení dat před selháním techniky (a samozřejmě nejen techniky) je **zálohování dat.** Principů zálohování dat je mnoho, záleží především na našich možnostech (zejména finančních):

- **on-line kopie disků** (mirroring) – pole RAID (drahé, ale velmi bezpečné),

- **příležitostná kopie dat** – kopírováním na záložní média (dnes zejména USB flash),
- **občasná bezpečnostní kopie dat** – např. automatické ukládání Office,
- **plánované kopie dat** – uživatelem naplánovaná úloha (MS Backup):
  - **kompletní** – obvykle všechny soubory i stav systému,
  - **denní** – soubory změněné v den, kdy bylo denní zálohování provedeno,
  - **rozdílové** – soubory vytvořené nebo změněné od posledního normálního nebo přírůstkového zálohování,
  - **přírůstkové** – soubory vytvořené nebo změněné od posledního normálního nebo přírůstkového zálohování, dále se však již nezálohují,
  - **normální** – zkopíruje všechny vybrané soubory a označí každý soubor jako zálohovaný.
- **uchování předchozích verzí souborů** (funkce některých OS) – umožňuje návrat zpět při zjištění chybných úprav.

Při zálohování jsou pak často využívány techniky:

- komprimace dat,
- vypalování dat,
- vytvoření kompletního obrazu (image) disku,
- klonování disku,
- outsourcing – vzdálené ukládání dat (FTP servery specializovaných firem).

Uvedené principy a metody zálohování je žádoucí kombinovat, např. mít data na poli RAID, ale občas pořídit i kopii důležitých dat na USB flash. Bezpečnost dat zvyšuje aktivní funkce uchování předchozích verzí souborů. Tím se lze elegantně ochránit i proti případné neopatrnosti při úpravách dokumentů.

3.3 Ochrana dat před dalšími vlivy

3.3.2 Endogenní vlivy

Havárie v důsledku endogenních (vnitřních) vlivů mají jednu charakteristickou vlastnost – nepředcházel jim žádný úmysl.

- **Vlivy lidského charakteru –** Nekompromisně nejdestruktivnějším faktorem pro PC je přesvědčení uživatele, že dané problematice rozumí, nezřídka kombinované s ochotou experimentovat a často pak i doprovázené zapomnětlivostí.
- **Jiné vlivy –** Faktor vycházející zevnitř systému. Můžeme sem zařadit selhání techniky v důsledku různých nedokonalostí programu, zjevných i skrytých závad atd.

3.3.1 Exogenní vlivy

Vedle plánovitých a vědomých útoků hrozí počítačové technice další nebezpečí, kterými jsou přírodní živly jako například požáry, zemětřesení nebo povodně. Těžko je možné ochránit PC dokonale proti běsnění živlů. S trochou předvídavosti a notnou dávkou štěstí mohou být zmírněny dopady těch snadněji předvídatelných, především bouřek. Nejběžnější a v tomto případě dokonce nejspolehlivější ochranou je odpojení PC a modemu od silových (230V) a komunikačních sítí (telefonní linka). Bohužel ne vždy je možné toto nebezpečí včas podchytit. Nezbývá než nespolehlivý lidský faktor nahradit technikou:

→ **UPS -** zkratka pochází ze slov „**Uninterruptible Power Supply**“, jedná se tedy o zařízení nebo systém zajišťující souvislou dodávku elektřiny pro zařízení, která nesmějí být neočekávaně vypnuta. V případě přerušení dodávky elektřiny zajistí napájení pro tyto přístroje a doba, po kterou udrží UPS zařízení v chodu, záleží na kapacitě akumulátorů a jiných parametrech.

Přerušení dodávky elektřiny z primárního zdroje může způsobit například ztráta napájení (blackout), dlouhodobé přepětí či rušení v síti (šum). Systém UPS je

obvykle využíván u nemocničních přístrojů, telekomunikačních zařízení nebo třeba systémů zajišťujících chod letišť. [22]

Ani UPS však není stoprocentní ochrana, proto je důležité nezapomínat a důležitá data poctivě zálohovat! Dojde-li i přes UPS k selhání techniky a následné ztrátě dat, je zálohování dat jediný možný způsob jejich záchrany.

4 KDYŽ JE POČÍTAČ INFIKOVÁN

4.1 Vlastní pomoc

Specifikem běžného českého uživatele PC je ojedinělá vlastnost dokázat si v krizové situaci velmi často pomoci svými vlastními prostředky. Důvod je možné spatřovat v omezených finančních prostředcích a zároveň v relativně vyspělé technologické úrovni společnosti. Nedisponuje-li přímo samotný uživatel nutnými odbornými znalostmi, zpravidla se v jeho blízkém okolí (spolužáci, kolegové, rodina) vyskytuje někdo na vyšší IT úrovni, který by mohl být schopen problém vyřešit. Negativem tohoto přístupu zůstává mnohdy neschopnost tohoto „amatérského odborníka“ zodpovědně posoudit své schopnosti, což mnohdy vede k pochybením (a následně ke škodám), kterých by se profesionál nedopustil.

Oprava svépomocí je obvykle realizována levnými, respektive volně šiřitelnými, prostředky (antivirovými systémy, detekčními a opravnými nástroji), které mají jen omezené funkce. Výsledkem opravy tedy často bývá sice fungující PC, bohužel nadále obsahující další neodhalené infekce. Nezřídka se uživatel musí smířit se ztrátou dat.

Veškeré výše popisované poznatky se opírají o zkušenosti a znalosti vycházející z mnohaleté praxe pracovníků jiříkovské firmy PC-info působící v oblasti správy sítí LAN.

4.2 Odborník

Možnosti běžného uživatele PC jsou pochopitelně omezené a je vhodné, aby uživatel včas zvážil, zda je v jeho silách situaci vyřešit, než (v dobré víře) způsobí ještě větší škodu. K odstranění závažných poruch PC a ke zpětnému získání dat by měli být povoláni odborníci nebo specializované firmy. Pro tyto případy jsou využívány odborné diagnostické a záchranné nástroje pro:

- detekci vad hardware (testy pamětí, VGA, zátěžové testy apod.),
- vyhledání a odstranění virů, spyware apod.,

- opravu chyb v registrech,
- obnovu smazaných dat,
- záchranu dat z poškozeného disku,
- opravu či reinstalaci OS a aplikací,
- zjištění zapomenutých hesel,
- zálohování dat (před opravou),
- zjištění konfigurace PC,
- stažení správných ovladačů periferií,
- a jiné potřebné utility.

Po zjištění závažné poruchy či ztráty dat je jediným správným řešením okamžité ukončení práce s PC, neboť každá další činnost výrazně snižuje možnost rekonstrukce funkčního stavu. Transport k odborníkovi, oprava závady a záchrana dat přirozeně bude finančně náročnější než oprava svépomocí. Náklady na záchranu dat se mohou orientačně pohybovat následovně:

Tabulka č. 1 Orientační ceník některých úkonů prováděných při záchraně dat

Orientační ceník některých úkonů prováděných při záchraně dat:	
Diagnostika vadného média	ZDARMA
Neúspěšná záchrana dat	0,- Kč
Oprava poškozených pcb	od 250,- Kč
Pájení a čipů v provedení BGA	od 500,- Kč
Rekonstrukce poškozených souborových systémů	od 350,- Kč
Demontáž zadřených ložisek motoru vřetene	od 2000,- Kč
Otevření disku a práce s plotnami v bezprašné komoře	od 900,- Kč
Vytvoření binární kopie mechanicky poškozeného povrchu plotny	od 1350,- Kč
Analýza a rekonstrukce poškozených servisních dat	od 800,- Kč
Oprava diskových polí RAID	individuálně
	Ceny jsou bez DPH

Zdroj: <www.datahelp.cz>

Tabulka č. 2 Orientační ceník konkrétních případů

Orientační ceník konkrétních případů:	
Pevné disky:	
Poškození souborového systému	od 900,- Kč
Poškozená elektronická část HDD	od 1500,- Kč
Poškození servisních dat, firmware	od 1500,- Kč
Mechanické poškození součástí disku	od 3000,- Kč
USB flash disky, paměťové karty:	
Poškození souborového systému	od 500,- Kč
Elektronické, mechanické poškození	od 1000,- Kč
Disková pole RAID	individuálně
	Ceny jsou bez DPH

Zdroj: <www.datahelp.cz>

Výše uvedené tabulky a data v nich obsažená (bez rozvinutí odborných termínů a zkratek) jsou výňatkem ceníku pražské společnosti DataHelp s.r.o.

5 DOTAZNÍK PREFERENCE UŽIVATELŮ V OBLASTI ZABEZPEČENÍ POČÍTAČE

5.1 Obsah dotazníku

V rámci mé bakalářské práce jsem vytvořila dotazník, jehož smyslem bylo zjistit aktuální situaci v povědomí uživatelů počítače o zabezpečení výpočetní techniky v jejich domácnosti. Cílovou skupinou pro tento dotazník se stali zaměstnanci veřejné správy v regionu Šluknovského výběžku. Jednalo se o zaměstnance městských, pracovních a finančních úřadů města Rumburka, Jiříkova a Varnsdorfu. Vzhledem k faktu, že na těchto pozicích pracují v drtivé většině ženy, jsou muži procentuálně zastoupeni v dotazníku pouze z 30 %. Nejpočetnější zastoupení zaznamenala věková skupina respondentů v rozmezí 24 let až 39 let v poměru 56 %. Druhou nejobsáhlejší skupinu 41 % tvoří respondenti ve věku 40 let až 59 let. Identifikace respondenta byla obsahem první části dotazníku.

Dotazník obsahuje celkem třicet otázek a byl sestaven do pěti částí dle zaměření jednotlivých otázek. Ve většině případů jsou u otázek uvedeny procentuální grafy. Dotazník byl distribuován prostřednictvím elektronické pošty v období mezi 21. únorem 2011 a 31. březnem 2011. Celkem se dotazníku zúčastnilo a otázky zodpovědělo 91 respondentů.

5.2 Vyhodnocení dotazníku

5.2.1 Technické vybavení respondenta

Následující údaje vycházejí z absolutních čísel uvedených v tabulce č. 3. Z výsledků šetření bylo prokázáno, že v jedné domácnosti je průměrně 2,6 počítačů nebo jiných podobných zařízení stejného charakteru (chytrý mobilní telefon s operačním systémem, tablet a jiné). Navíc na jednu domácnost připadá průměrně 2,9 uživatelů těchto zařízení. Tyto poznatky prokázaly, že jeden počítač v každé domácnosti používá průměrně 1,1 uživatel.

Z celkového počtu 91 respondentů 25 % odpovědělo, že se v jejich domácnosti nachází jeden nebo více zařízení s nelegálním operačním systémem. 14 % počítačů nebo jiných podobných zařízení stejného charakteru je vybaveno nelegálním operačním systémem. Pozitivním výstupem šetření je fakt, že 82 % zařízení je vybaveno prostředky ochrany výpočetní techniky (antivirový software, zálohování dat a jiné).

Tabulka č. 3 Výsledky druhé části dotazníku nazvané „Technické vybavení respondenta“

Otázka	Celkový počet
2.1 Kolik se ve Vaší domácnosti vyskytuje uživatelů počítače a jiných podobných zařízení?	262
2.2 Kolik se ve Vaší domácnosti vyskytuje počítačů a jiných podobných zařízení stejného charakteru?	233
2.3 Kolik z Vašich zařízení je vybaveno nelegálním operačním systémem?	33
2.4 Kolik z Vašich zařízení je vybaveno prostředky ochrany výpočetní techniky?	192

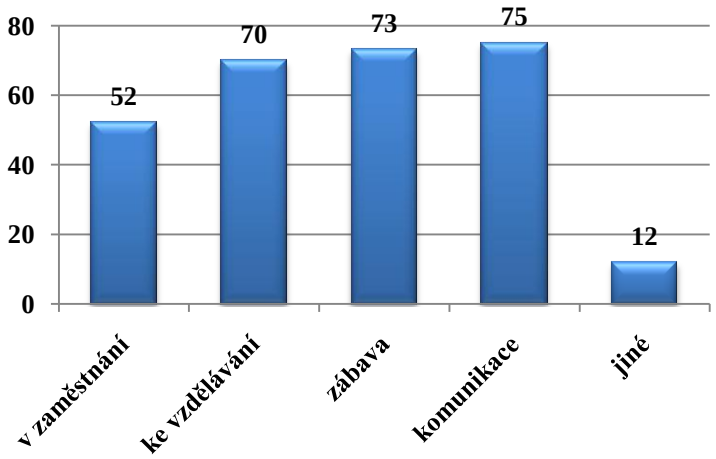
Zdroj: vlastní šetření

.2.2 Stav ochrany PC

Otázka 3.1 zjišťovala, za jakým účelem používají uživatelé svůj počítač. Celkem odpovídalo 91 respondentů. U této otázky bylo možno označit více správných odpovědí. Z výsledků vyplývá, že pro počítačové uživatele jsou důležitými faktory především komunikace s okolním světem (75 respondentů z 91 takto odpovědělo) a hned poté zábava (odpovědělo 73 respondentů z 91). Přístup k informacím a tedy přístup k sebevzdělávání je důležitý pro 70 respondentů z 91. Celkem 51 respondentů odpovědělo, že svůj počítač používají také v zaměstnání. 12 respondentů vybralo možnost jiné a odpovídali vlastními slovy. Mezi tyto odpovědi patřil např. nákup a prodej zboží přes internet, rezervace vstupenek, ale i stahování hudby. Zbylých 5 respondentů odpovědělo, že si na internetu vyhledávají informace např. o bydlení, cestování, vaření apod.

Z výsledků tedy vyplývá, že u většiny respondentů jsou seriózní účely počítače (zaměstnání, platební styk, vzdělávání) kombinovány s komunikací a zábavou (facebook, stahování hudby a jiné), což může představovat významné bezpečnostní riziko.

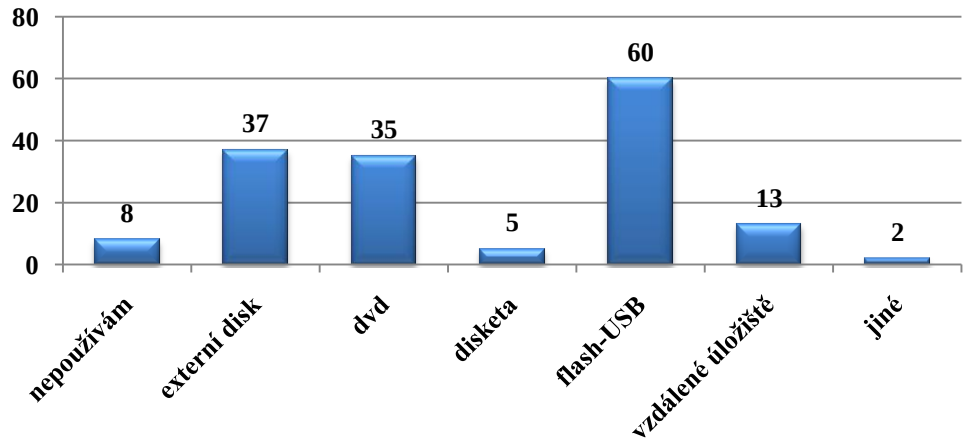
Graf 3. 1 K jakým účelům využíváte především svůj počítač?



Otázka zálohování dat byla předmětem dalšího dotazu. Konkrétně se týkala preferencí uživatelů na systémy pro zálohování důležitých dat. Celkem odpovídalo 91 respondentů. U této otázky bylo taktéž možno označit více správných odpovědí. Největší počet, 60 respondentů z 91, pro zálohování dat používá USB flash. Na druhém a třetím místě se umístilo zálohování prostřednictvím externího disku a dvd (72 respondentů z 91). 13 respondentů používá vzdálené úložiště, tzv. cloud a jen 5 respondentů zálohuje na diskety. Dva respondenti vybrali možnost jiné a jejich odpovědi jsou FTP a ukládání dat do emailových zpráv. Pouhých 8 respondentů odpovědělo, že svá data vůbec nezálohují.

Z šetření bylo zjištěno, že většina respondentů používá pro zálohování dat USB flash, což se ve spojení s faktem, že USB flash používají pro kontakt s jinými PC a zpravidla nedbale realizují jeho antivirovou kontrolu (viz otázka 3.8), ukazuje jako nejméně vhodný výběr záložního média.

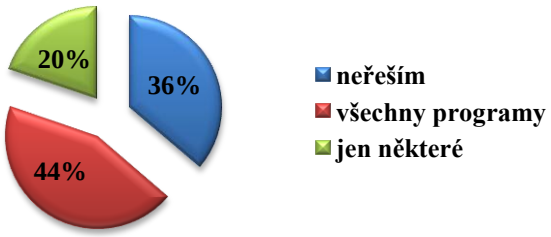
Graf 3. 2 Jaký používáte systém pro zálohování důležitých dat?



Otázka 3.3 se týkala aktualizací OS a jiných aplikací. Většina respondentů (44 %) aktualizuje pravidelně všechny programy a aplikace. Ovšem 36 % respondentů, se o tuto problematiku vůbec nestará a aktualizace neřeší. Vzhledem k tomu, o jak velké procentuální zastoupení se jedná, je zjištěná skutečnost alarmující.

V naprosté většině bylo prokázáno, že jde o respondenty, kteří používají nelegální software (zejména OS Windows) a mají obavy z možného zablokování Windows po aktualizaci. Prokazatelná je tedy závislost: nelegální software -> chybějící aktualizace -> vysoké bezpečnostní riziko.

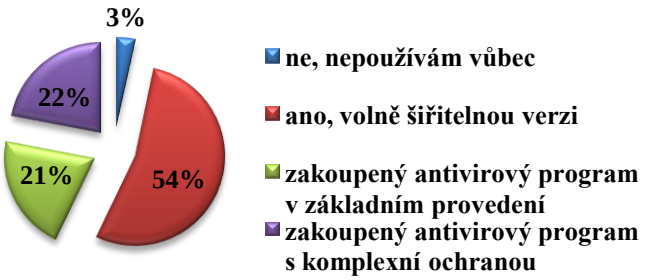
Graf 3. 3 Aktualizujete pravidelně operační systém a aplikace ve Vašem počítači?



V otázce 3.4 byli respondenti dotazováni, zda používají antivirový program. Více jak polovina respondentů využívá volně šiřitelnou verzi antivirového programu. 21 % respondentů vlastní zakoupený antivirový program v základním provedení a dalších 22 % vlastní zakoupený antivirový program s komplexní ochranou, tzn. včetně firewallu, antispamu a jiných.

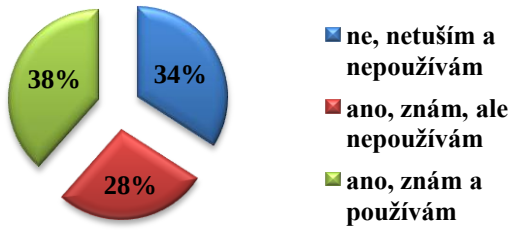
V souvislosti s tím, že volně šiřitelné verze antivirového programu a antivirové programy v základním provedení zpravidla řeší jen základní ochranu PC, je možno konstatovat, že 78 % respondentů nemá dostatečně zabezpečenou techniku.

Graf 3. 4 Používáte antivirový program? Pokud ano, v jakém rozsahu?



Otázka 3.5 byla zaměřena na ochranu počítače před útoky ze sítě. Firewall je nástroj, který blokuje podezřelá spojení a kontroluje komunikaci mezi počítačem uživatele a okolními počítači. Z výsledků šetření je patrné, že 38 % respondentů používá firewall. Takto vysoké procento je pozitivní jev. Skupina respondentů, kteří sice vědí, co pojem firewall znamená a jaké jsou jeho funkce, ale nepoužívají jej, čítá 28 %. Motivem nepoužití firewallu může být mylná představa o výši ceny takto vybaveného antivirového systému. V případě vyšší informovanosti uživatelů počítačů o přibližných cenách kvalitní antivirové ochrany by uvedených 28 % respondentů jistě bylo ochotno firewall zakoupit a používat.

Graf 3. 5 Víte zhruba, co je to firewall? Používáte firewall?



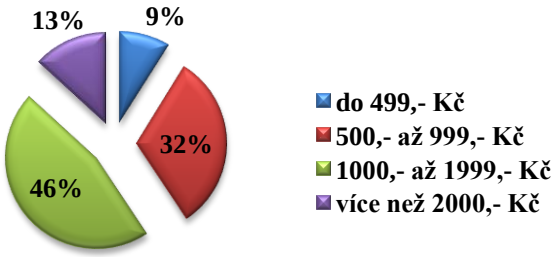
Následující dvě otázky se týkaly stejné záležitosti, ale zjišťovaly odlišné pohledy. Otázka 3.6 zjišťovala, jakou má uživatel představu o ceně kompletní ochrany PC na jeden rok. Pro 46 % respondentů se tato položka pohybuje mezi 1000,- Kč a 1999,- Kč.

Zjištění z této otázky jednoznačně prokazuje souvislost mezi informovaností o ceně antivirového systému (41 % respondentů má správnou představu) a používáním kompletní antivirové ochrany (38 % respondentů z otázky 3.5).

Otázka 3.6 ukazuje katastrofální neinformovanost prakticky poloviny respondentů o cenách kompletních antivirových systémů na našem trhu. Předpokládáme-li, že se v běžné domácnosti nacházejí tři počítače nebo podobná zařízení stejného charakteru (v druhé části dotazníku nazvané „Technické vybavení respondenta“ byl zjištěn průměrný počet počítačů 2,6 v jedné domácnosti), pak se

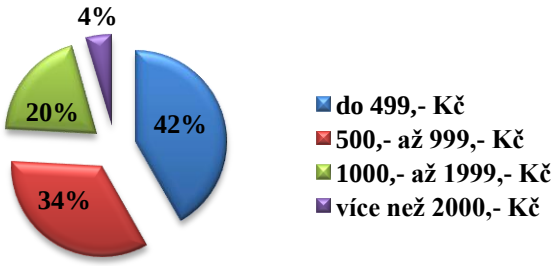
může cena přechodu ke kompletnímu antivirovému systému při nákupu na dvouleté období pohybovat okolo 367,- Kč pro jednu licenci na jeden rok. [10]

Graf 3. 6 Kolik myslíte, že stojí kompletní ochrana počítače na dobu jednoho roku?



Naproti tomu otázka 3.7 zjišťovala, jakou částku jsou uživatelé ochotni investovat do kompletní ochrany PC na dobu jednoho roku. Průzkumem v této otázce bylo zjištěno, že 76 % respondentů by mohlo používat při správné informovanosti kvalitní antivirovou ochranu. Počet komplexně chráněných PC by se tak zcela jistě zdvojnásobil.

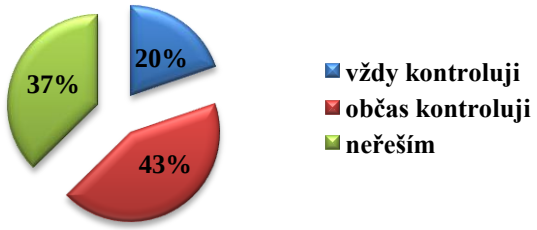
Graf 3. 7 Kolik byste byli ochotni investovat do ochrany počítače na dobu jednoho roku?



Další otázka se dotazovala respondentů, zda kontrolují USB flash disk, který připojují ke svému PC. Vysoké číslo 37 % respondentů žádným způsobem prověření USB flash disku neřeší. Přitom tento způsob zálohy dat obvykle plní uživateli

několik dalších funkcí, a to například přenos dokumentů na jiné PC a bývá zde uložen certifikát pro platební styk. Až 80 % respondentů nevěnuje kontrole USB flash disku dostatečnou pozornost.

Graf 3. 8 Kontrolujete vložený USB flash?



V otázce 3.9 odpovídali respondenti na dotaz, jakým způsobem nakládají s nevyžádanou poštou. Zjištění, že nikdo z dotázaných respondentů nepřeposílá spam, je velmi pozitivní. Zvědavost 5 % respondentů, kteří spam před smazáním přečtou, je pochopitelná a není reálný předpoklad snížení tohoto počtu uživatelů.

Graf 3. 9 Jakým způsobem nakládáte s tzv. spamem (nevyžádanou poštou)?

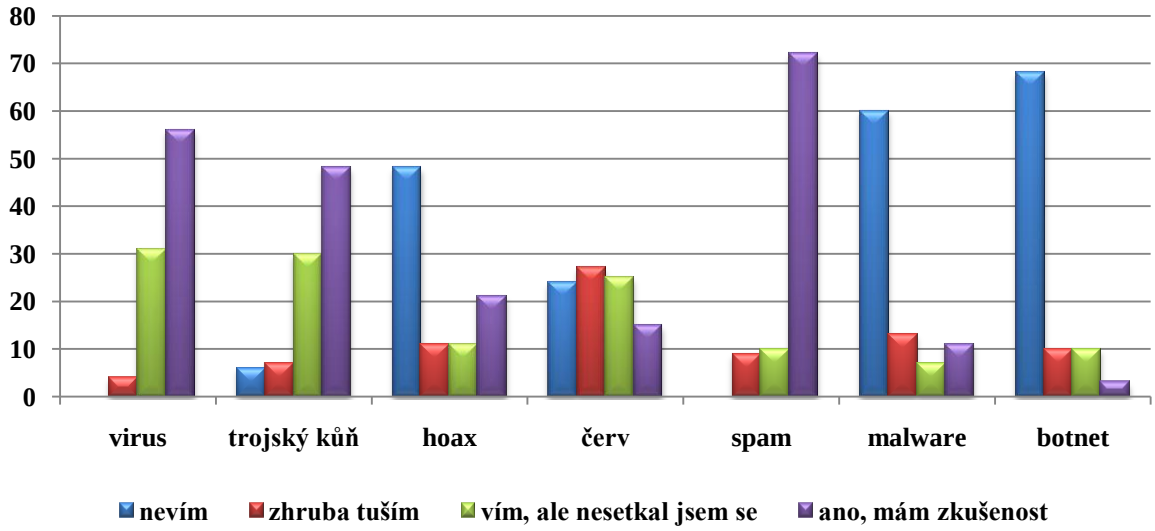
5.2.3 Orientace respondenta v terminologii

Ve čtvrté části dotazníku bylo zjišťováno, do jaké míry respondenti znají a chápou význam sedmi vybraných nejčastěji používaných termínů úzce souvisejících s oblastí počítačové bezpečnosti. Na těchto sedm otázek odpovídalo

celkem 91 respondentů. Údaje v grafu jsou uvedeny v absolutních číslech. Šetřením bylo prokázáno, že nejlépe se respondenti orientují v pojmech virus, trojský kůň a spam. Velký počet respondentů se doposud nesetkal s označením hoax a malware. Pro značnou část respondentů (68 respondentů z 91) je pojem botnet neznámý.

Výsledky šetření nejsou žádným způsobem překvapující. Reprezentují poměrně dobrou počítačovou gramotnost populace.

Graf 4 Máte představu o významu následujících pojmů nebo setkali jste se s následujícími pojmy?



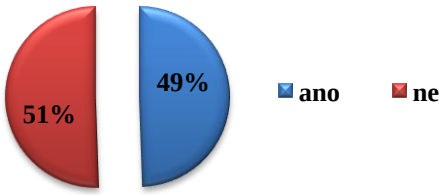
5.2.4 Zkušenosti respondenta

Otázka 5.1 se týkala zkušenosti uživatelů s potenciálně nebezpečnými internetovými stránkami. Tyto stránky mohou být například stránky šířící násilí, stránky s nelegálním software ke stažení, stránky s pornografickou tématikou a mnoho dalších stránek pohybujících se na hraně současné legislativy. Každý uživatel se někdy setká s odkazem na takovéto „pochybné“ stránky, ale jejich prohlížení znamená určité bezpečnostní riziko.

Téměř polovina (49 %) respondentů má tedy zkušenost s potenciálně škodlivými stránkami a byla by pro ně prokazatelně přínosná existence komplexní antivirové ochrany vybavené kvalitním firewallem. Ve skutečnosti může být počet

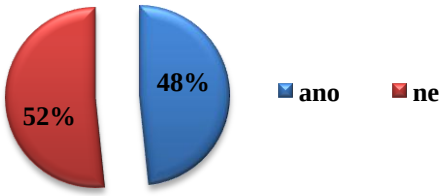
uživatelů, kteří se setkali s infikovanou internetovou stránkou mnohem vyšší, neboť většina běžných uživatelů (amatérů) toto nebezpečí ani nezaregistruje.

Graf 5. 1 Setkali jste se již někdy s internetovou stránkou, jejíž obsah mohl být potenciálně škodlivý?



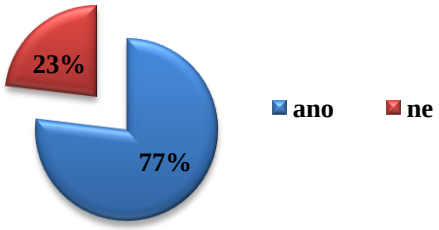
V otázce 5.2 byli respondenti dotazováni na svou zkušenost s infikovaným médiem. Celých 48 % respondentů odpovědělo kladně. Když tento poznatek dáme do souvislosti s výsledky otázky 3.8, tedy že sice skoro celá polovina respondentů přišla do styku s infikovaným médiem, ale jen 20 % respondentů vložený USB flash disk vždy kontroluje, je prokázáno vysoké potenciální nebezpečí s možným následkem velkých škod. Zjištění z této otázky je podobné jako u otázky 5.1, přičemž je předpoklad, že z oněch 52 % respondentů většina nákazu nezjišťovala a tudíž ani nezaregistrovala.

Graf 5. 2 Setkali jste se již někdy s napadeným médiem?



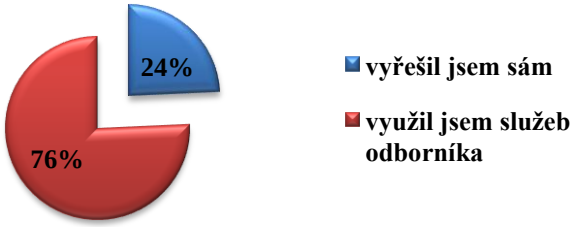
Otázka 5.3 se zaměřila na zkušenosti uživatelů v případě selhání techniky. 77 % respondentů odpovědělo, že se s těmito problémy již setkalo. Zjištění z této otázky bylo překvapivé a jednoznačně ukazuje, že závažné problémy končící mnohdy i ztrátou dat se uživatelům rozhodně nevyhýbají. Pozitivní na tomto faktu může být, že se zvyšující informovaností uživatelů PC a postupným růstem důležitosti techniky se vytváří tlak na příslušná preventivní opatření.

Graf 5. 3 Setkali jste se u sebe nebo u někoho ve svém okolí se závažnými problémy v souvislosti se selháním techniky?



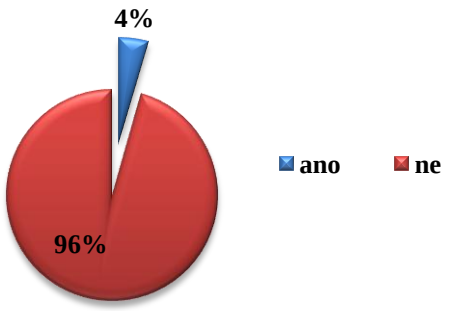
Otázka 5.4 má přímou souvislost s otázkou 5.3 a tuto otázku zodpovídali pouze ti uživatelé, kteří v předchozí otázce odpověděli kladně. Pouze 24 % respondentů vyřešilo problémy s PC svépomocí. 76 % respondentů pak bylo nuceno využít služeb odborníka. 24 % respondentů disponujících potřebnými odbornými znalostmi může být na jedné straně lichotivé procento populace, na druhé straně je však nutno si uvědomit, že takto vysoké procento uživatelů je k opravě svépomocí přinuceno zejména z finančních důvodů.

Graf 5. 4 Jakým způsobem byl problém řešen?



U předposlední otázky byla pozornost věnována zkušenostem respondenta s policejním vyšetřováním v oblasti PC bezpečnosti. Celá 4 % respondentů se s výše popisovanou situací setkalo. Zjištění otázky 5.6 potvrzuje, že počítačová kriminalita je aktuálním a ožehavým problémem současnosti.

Graf 5. 6 Setkali jste se již někdy s policejním vyšetřováním v oblasti počítačové bezpečnosti (napadení počítače hackrem, nelegální software)?



Poslední otázka 5.7 se dotazovala, zda se respondent setkal s jiným narušením bezpečnosti počítače a dat, než bylo uvedeno v dotazníku. Otázka byla zařazena jen pro uživatele, kteří by nepovažovali tento dotazník za plně vyčerpávající jejich zkušenosti a potřebovali nám sdělit svůj závažný poznatek. Pouze 3 respondenti tuto možnost využili, většina respondentů neměla potřebu dotazník doplnit.

5.3 Shrnutí dotazníku

V první řadě je možno říct, že až na drobné odchylky se potvrdil předpokládaný výsledek dotazníku. Respondenti se velmi uspokojivě orientují v obecných pojmech v oblasti počítačové bezpečnosti. Ovšem je nutná také ostražitost před novými hrozbami, které v dané oblasti v poslední době vznikají a jejich zvyšující nebezpečnost někteří uživatelé nezaregistrovali. Šetřením byla prokázána souvislost mezi informovaností o cenách antivirových systémů a používáním komplexní antivirové ochrany. Je možno konstatovat, že se zvýšením

informovanosti by došlo ke zvýšení procenta uživatelů, kteří by svůj počítač komplexně chránili. Z výsledků šetření je nutno poukázat na nevhodnost výběru prostředku pro zálohování dat, kdy naprostá většina uživatelů volí pro tyto účely USB flash, v souvislosti s nedostatečnou kontrolou toho prostředku. Tyto výsledky potom jen potvrzuje zjištění, že velká skupina respondentů se setkala s infikovaným USB flash. Dopady této nedostatečné obezřetnosti jsou často následné selhání techniky a ztráta dat. Nad očekávání velká část uživatelů utrpěla významnou škodu v důsledku selhání techniky, kdy se přímá i nepřímá finanční ztráta pohybovala v řádech tisíců Kč.

ZÁVĚR

Počítačová bezpečnost je oborem informatiky zabývající se zabezpečením informací v počítačích. Tato úloha spočívá ve třech krocích, a to v prevenci, v detekci a v nápravě. Úkolem počítačové bezpečnosti je například ochrana před neoprávněnou manipulací s informacemi, ochrana informací před krádeží či poškozením nebo bezpečné zálohování dat. Hlavní snahou mé bakalářské práce bylo přiblížit tento rozsáhlý a odborně poměrně náročný obor běžnému uživateli počítače.

V teoretické části, a to v druhé a třetí kapitole, jsem se snažila popsat všechny hrozby, které se mohou dotýkat uživatelů počítače, a naproti nim postupy, kterými lze zvýšit míru zabezpečení počítače. Další kapitoly mají již praktický charakter. Čtvrtá kapitola se zabývá možnostmi výše zmíněné nápravy v případě, kdy již byl počítač infikován. V praxi lze uvažovat pouze dvě varianty jak odstranit potíže spojené s napadeným počítačem, a to řešit situaci svépomocí nebo infikovaný počítač svěřit odborníkům. Výsledné rozhodnutí závisí na úrovni schopností a zkušeností uživatele, ale také na jeho finanční situaci. Jak bylo prokázáno na základě dotazníkového šetření v páté kapitole, značné procento uživatelů si dokáže v takovéto krizové situaci poradit bez odborné spolupráce. Zda je tento fakt důsledkem nepříznivé finanční situace nelze už doložit. Již jsem zmínila obsah páté kapitoly, tedy analýzu výsledků dotazníku, který jsem vytvořila v rámci této práce. Dotazník byl zaměřen na otázky týkající se znalostí a preferencí počítačových uživatelů v oblasti zabezpečení počítače.

Zjištěný fakt, že uživatelská orientace v dané problematice je na poměrně vysoké úrovni, považuji za velmi příznivý. Nicméně by bylo jen ku prospěchu věci, kdyby se zlepšila osvěta vzhledem k hrozbám, které v souvislosti s počítačovou bezpečností vyvstávají až v poslední době. Negativním jevem je prokázaná zkreslenost představ uživatelů o cenách produktů antivirové ochrany dostupných na trhu. Bylo prokázáno, že kvalitní komplexní systémy v plné verzi nejsou využívány především z důvodu nedostatečné informovanosti uživatelů o cenách těchto produktů. Aplikace výše uvedených poznatků v praxi by mohla být podkladem kampaně za vyšší úroveň informovanosti populace České republiky

v dané problematice. Každý uživatel počítače je v dnešní době především uživatelem internetu a měl by si uvědomit, že pocit anonymity a bezpečí je falešný, a začít se maximální měrou aktivně podílet na ochraně svého soukromí.

SEZNAM POUŽITÉ LITERATURY

[1] Antivirové centrum [online]. [cit. 2011-03-30]. Dostupné z: <http://www.antivirovecentrum.cz/>.

[2] *Ceník záchrany dat* [online]. [cit. 2011-03-17]. Dostupné z: <http://www.datahelp.cz/cenik-zachrany-dat/>.

[3] Časová osa Chipu: Počítačové viry [online]. [cit. 2011-03-31]. Dostupné z: <http://earchiv.chip.cz/cs/earchiv/vydani/r-2009/coc-pocitacove-viry.html>.

[4] ČEPELÁK, Ondřej. *Druhy počítačových virů* [online]. 19. 2. 2010, [cit. 2011-1-3]. Dostupné z: <http://www.pcporadenstvi.cz/druhy-pocitacovych-viru>.

[5] DOSTÁLEK, L. A KOL. *Velký průvodce protokoly TCP/IP: Bezpečnost.* Brno: Computer Press, 2006. ISBN 80-7226-849-X.

[6] DŽUBÁK, J. *Co je to hoax* [online]. [cit. 2011-03-17]. Dostupné z: <http://www.hoax.cz/hoax/co-je-to-hoax>.

[7] DŽUBÁK, J. *Co je to phishing* [online]. [cit. 2011-03-17]. Dostupné z: <http://www.hoax.cz/phishing/co-je-to-phishing>

[8] ENDORF, C. *Detekce a prevence počítačového útoku.* 1. vyd. Praha: Grada, 2005. ISBN 80-247-1035-8.

[9] HÁK, I. *Moderní počítačové viry, třetí vydání* [online]. [cit. 2011-03-17]. Dostupné z: <http://www.viry.cz/viry.cz/kniha/kniha.pdf>.

[10] *Kaspersky Lab - eShop* [online]. [cit. 2011-04-15]. Dostupné z: <http://www.kaspersky.cz/eshop/vse/>.

[11] KLEGA, Vratislav. Počítač trucuje. Není hacknutý?. *CHIP: magazín informačních technologií*, listopad 2010, ročník 20, č. 12, s. 60-63. ISSN 1210-0684.

[12] KOLÁČEK, M. *Počítačová havěť - vývoj a rozdělení malware* [online]. 12. února 2009, [cit. 2011-03-17]. Dostupné z: <http://www.svethardware.cz/art_doc-60AE8EC866175F58C12575550027B353.html>.

[13] KRÁL, M. *Bezpečnost domácího počítače prakticky a názorně.* 1. vyd. Praha: Grada Publishing, 2006. 366 s. ISBN 80-247-1408-6.

[14] KRATOCHVÍL, P. *2009: Rok supervirů* [online]. [cit. 2011-03-20]. Dostupné z: <http://earchiv.chip.cz/cs/earchiv/autor/kratochvil-petr/rok2009-superviru.html>.

[15] NAMESTNIKOVA, M. *Spam report: January 2011* [online]. [cit. 2011-03-17]. Dostupné z: <http://www.securelist.com/en/analysis/204792164/Spam_report_January_2011>.

[16] NAVRÁTIL, P. *S počítačem nejen k maturitě.* 5. vyd. Kralice na Hané: Computer Media, 2004. ISBN 80-86686-20-5.

[17] NORTHCUTT, S. *Bezpečnost počítačových sítí.* Brno: Computer Press, 2006. ISBN 80-251-0697-7.

[18] ODEHNAL, P. *Praktická sebeobrana proti virům.* 1. vyd. Praha: Grada, 1996. 115 s. ISBN 80-7169-363-4.

[19] *The WildList Organization International* [online]. [cit. 2011-1-3]. Dostupné z: <http://www.wildlist.org/>.

[20] THOMAS, T. M. *Network Security First-Step.* Cisco Press, 2004. ISBN 1-58720-099-6.

[21] *Top 10 Antivirus Protection* [online]. [cit. 2011-04-15]. Dostupné z: <http://www.top10list.com/top,10,antivirus,protection/top-ten-antivirus-protection.asp>.

[22] VITOVSKÝ, A. *Moderní slovník softwaru.* 1. vyd. Praha: Antonín Vitovský - AV SOFTWARE, 2006. 588 s. ISBN 80-901428-8-5.

[23] ZAKORZHEVSKY, V. *Monthly Malware Statistics, February 2011* [online]. [cit. 2011-03-17]. Dostupné z: <http://www.securelist.com/en/analysis/204792166/Monthly_Malware_Statistics_February_2011>.

PŘÍLOHY

Příloha č. 1: Dotazník pro soukromé šetření k bakalářské práci.

Příloha č. 2: Tabulka č. 1: Výsledky dotazníku pro soukromé šetření.

Příloha č. 3: Top 10 Antivirus Protection – seznam nejlepších produktů antivirové ochrany sestavený webovým serverem TopList.com.

Příloha č. 1

DOTAZNÍK PRO SOUKROMÉ ŠETŘENÍ

1. IDENTIFIKACE RESPONDENTA

1.1. Věková kategorie

- ○ do 24 let
- ○ 24 - 39 let
- ○ 40 - 59 let
- ○ nad 60 let

1.2. Pohlaví

- ○ žena
- ○ muž

1.3. Zaměstnání

- ○ student
- ○ zaměstnanec
- ○ podnikatel
- ○ důchodce
- ○ nezaměstnaný
- ○ jiné (doplňte): ☐

2. TECHNICKÉ VYBAVENÍ RESPONDENTA

2.1. Kolik se ve Vaší domácnosti vyskytuje uživatelů počítače a jiných podobných zařízení (chytrý mobilní telefon s operačním systémem, tablet a jiné)?

☐

2.2. Kolik se ve Vaší domácnosti vyskytuje počítačů a jiných podobných zařízení stejného charakteru (chytrý mobilní telefon s operačním systémem, tablet a jiné)?

☐

2.3. Kolik z Vašich zařízení je vybaveno nelegálním operačním systémem (tzv. kopírovanými Windows)?

☐

2.4. Kolik z Vašich zařízení je vybaveno prostředky ochrany výpočetní techniky (antivirový software, zálohování dat a jiné)?

☐

3. STAV OCHRANY PC

3.1. K jakým účelům využíváte především svůj počítač? (zde může být označeno více správných odpovědí)

- ☐ v zaměstnání
- ☐ ke vzdělávání
- ☐ zábava
- ☐ komunikace
- ☐ jiné (doplňte): ☐

3.2. **Jaký používáte systém pro zálohování důležitých dat?** (zde může být označeno více správných odpovědí)

- ☐ nepoužívám
- ☐ externí disk
- ☐ dvd
- ☐ disketa
- ☐ flash-USB
- ☐ vzdálené úložiště
- ☐ jiné (doplňte): _____

3.3. **Aktualizujete pravidelně operační systém a aplikace ve Vašem počítači (týká se Windows, internetových prohlížečů, aplikací Adobe Reader apod.)?**

- ○ neřeším
- ○ všechny programy
- ○ jen některé (doplňte): _____

3.4. **Používáte antivirový program? Pokud ano, v jakém rozsahu?**

- ○ ne, nepoužívám vůbec
- ○ ano, volně šiřitelnou verzi
- ○ zakoupený antivirový program v základním provedení
- ○ zakoupený antivirový program s kompletní ochranou (antivirový program, firewall, antispam apod.)

3.5. **Víte, co to je firewall? Používáte firewall?**

- ○ ne, nevím a nepoužívám
- ○ ano, znám, ale nepoužívám (různé důvody, např. cena apod.)
- ○ ano, znám a používám

3.6. **Kolik myslíte, že stojí kompletní ochrana počítače na dobu jednoho roku?**

- ○ do 499,- Kč
- ○ 500,- až 999,- Kč
- ○ 1000,- až 1999,- Kč
- ○ více než 2000,- Kč

3.7. **Kolik byste byli ochotni investovat do ochrany počítače na dobu jednoho roku?**

- ○ do 499,- Kč
- ○ 500,- až 999,- Kč
- ○ 1000,- až 1999,- Kč
- ○ více než 2000,- Kč

3.8. **Kontrolujete vložený USB flash?**

- ○ vždy kontroluj
- ○ občas kontroluji
- ○ neřeším

3.9. **Jakým způsobem nakládáte s tzv. spamem (nevyžádanou poštou)?**

- ○ mažu ihned bez přečtení
- ○ přečtu a poté smažu
- ○ přeposílám dál

4. ORIENTACE RESPONDENTA V TERMINOLOGII

Máte představu o významu následujících pojmů nebo setkali jste se s následujícími pojmy?

4.1. virus
- nevím
- zhruba tuším
- vím, ale nesetkal jsem se
- ano, mám zkušenost

4.2. trojský kůň
- nevím
- zhruba tuším
- vím, ale nesetkal jsem se
- ano, mám zkušenost

4.3. hoax
- nevím
- zhruba tuším
- vím, ale nesetkal jsem se
- ano, mám zkušenost

4.4. červ
- nevím
- zhruba tuším
- vím, ale nesetkal jsem se
- ano, mám zkušenost

4.5. spam
- nevím
- zhruba tuším
- vím, ale nesetkal jsem se
- ano, mám zkušenost

4.6. malware (všeobecně)
- nevím
- zhruba tuším
- vím, ale nesetkal jsem se
- ano, mám zkušenost

4.7. botnet
- nevím
- zhruba tuším
- vím, ale nesetkal jsem se
- ano, mám zkušenost

5. **ZKUŠENOSTI RESPONDENTA**

5.1. **Setkali jste se již někdy s internetovou stránkou, jejíž obsah mohl být potenciálně škodlivý? Chcete-li, upřesněte.**

- ○ ano, konkrétně (nepovinné):
- ○ ne

5.2. **Setkali jste se již někdy s napadeným médiem (zavlrovaný USB flash)?**

- ○ ano
- ○ ne

5.3. **Setkali jste se u sebe nebo u někoho ve svém okolí se závažnými problémy v souvislosti se selháním techniky (selhání počítače, ztráta dat a jiné)?**

- ○ ano
- ○ ne

5.4. **Jakým způsobem byl problém řešen?** (odpovídejte pouze v případě, že jste v otázce 5.3 odpověděli „ano")

- ○ vyřešil/a jsem si/vyřešili jsme si/vyřešili jsme
- ○ využil/a jsem služeb odborníka

5.5. **Na kolik byste zhruba vyčíslili přímou i nepřímou finanční ztrátu (nepřímou finanční ztrátou je myšlena nemožnost používat techniku)?** (odpovídejte pouze v případě, že jste v otázce 5.3 odpověděli „ano")

- ○ vyřešil/a jsem si/vyřešili jsme si/vyřešili jsme, a to odhadu: _____ Kč
- ○ využil/a jsem služeb odborníka, stálo to: _____ Kč

5.6. **Setkali jste se již někdy s policejním vyšetřováním v oblasti počítačové bezpečnosti (napadení počítače hackrem, nelegální software)?**

- ○ ano
- ○ ne

5.7. **Setkali jste se s jiným narušením bezpečnosti počítače a dat než zde bylo uvedeno?**

- ○ ne
- ○ ano (chcete-li, pošlete zrovna stručně svoji zkušenost):

Děkuji Vám za ochotu a čas věnovaný vyplnění dotazníku. Pokud jste při vyplňování dotazníku narazili na jakoukoli nesrovnalost, nebo máte jakékoli jiné dotazy či připomínky, uvítám zpětnou odezvu.

Vyplněný dotazník prosím uložte a odešlete zpět na adresu andrea.jaulhankova@fsv.cz jako přílohu elektronické pošty. Můžete použít i tlačítko v pravém horním rohu formuláře, které připraví zprávu s touto přílohou automaticky (ne na všech PC to musí fungovat).

Příloha č. 2

Otázka	Slovně	Odpověď	Počet
1. IDENTIFIKACE RESPONDENTA			
1.1.	Věková kategorie	do 24 let	2
		24 - 39 let	51
		40 - 59 let	37
		nad 60 let	1
1.2.	Pohlaví	žena	64
		muž	27
1.3.	Zaměstnání	student	0
		zaměstnanec	91
		podnikatel	0
		důchodce	0
		nezaměstnaný	0
		jiné	0
2. TECHNICKÉ VYBAVENÍ RESPONDENTA			
2.1.	Kolik se ve Vaší domácnosti vyskytuje uživatelů počítače a jiných podobných zařízení (chytrý mobilní telefon s operačním systémem, tablet a jiné)?		262
2.2.	Kolik se ve Vaší domácnosti vyskytuje počítačů a jiných podobných zařízení stejného charakteru (chytrý mobilní telefon s operačním systémem, tablet a jiné)?		233
2.3.	Kolik z Vašich zařízení je vybaveno nelegálním operačním systémem (tzv. kopírovanými Windows)?		33
2.4.	Kolik z Vašich zařízení je vybaveno prostředky ochrany výpočetní techniky (antivirový software, zálohování dat a jiné)?		192
3. STAV OCHRANY PC			
3.1.	K jakým účelům využíváte především svůj počítač?	v zaměstnání	52
		ke vzdělávání	70
		zábava	73
		komunikace	75
		jiné	12
3.2.	Jaký používáte systém pro zálohování důležitých dat?	nepoužívám	8
		externí disk	37
		dvd	35
		disketa	5
		flash-USB	60
		vzdálené úložiště	13
		jiné	2
3.3.	Aktualizujete pravidelně operační systém a aplikace ve Vašem počítači (týká se Windows, internetových prohlížečů, aplikací Adobe apod.)?	neřeším	33
		všechny programy	40
		jen některé	18
3.4.	Používáte antivirový program? Pokud ano, v jakém rozsahu?	ne, nepoužívám vůbec	3
		ano, volně šiřitelnou verzi	49
		zakoupený	19

		antivirový program v základním provedení	
		zakoupený antivirový program s komplexní ochranou	20
3.5.	Víte zhruba, co je to firewall? Používáte firewall?	ne, netuším a nepoužívám	31
		ano, znám, ale nepoužívám	25
		ano, znám a používám	35
3.6.	Kolik myslíte, že stojí kompletní ochrana počítače na dobu jednoho roku?	do 499,- Kč	8
		500,- až 999,- Kč	29
		1000,- až 1999,- Kč	42
		více než 2000,- Kč	12
3.7.	Kolik byste byli ochotni investovat do ochrany počítače na dobu jednoho roku?	do 499,- Kč	38
		500,- až 999,- Kč	31
		1000,- až 1999,- Kč	18
		více než 2000,- Kč	4
3.8.	Kontrolujete vložený USB flash?	vždy kontroluji	18
		občas kontroluji	39
		neřeším	34
3.9.	Jakým způsobem nakládáte s tzv. spamem (nevyžádanou poštou)?	mažu ihned bez přečtení	86
		přečtu a poté smažu	5
		přeposílám dál	0
4.	ORIENTACE RESPONDENTA V TERMINOLOGII		
4.1.	Virus	nevím	0
		zhruba tuším	4
		vím, ale nesetkal jsem se	31
		ano, mám zkušenost	56
4.2.	Trojský kůň	nevím	6
		zhruba tuším	7
		vím, ale nesetkal jsem se	30
		ano, mám zkušenost	48
4.3.	Hoax	nevím	48
		zhruba tuším	11
		vím, ale nesetkal jsem se	11
		ano, mám zkušenost	21
4.4.	Červ	nevím	24
		zhruba tuším	27

		vím, ale nesetkal jsem se	**25**
		ano, mám zkušenost	**15**
4.5.	**Spam**	**nevím**	**0**
		zhruba tuším	**9**
		vím, ale nesetkal jsem se	**10**
		ano, mám zkušenost	**72**
4.6.	**Malware (všeobecně)**	**nevím**	**60**
		zhruba tuším	**13**
		vím, ale nesetkal jsem se	**7**
		ano, mám zkušenost	**11**
4.7.	**Botnet**	**nevím**	**68**
		zhruba tuším	**10**
		vím, ale nesetkal jsem se	**10**
		ano, mám zkušenost	**3**
5. ZKUŠENOSTI RESPONDENTA			
5.1.	**Setkali jste se již někdy s internetovou stránkou, jejíž obsah mohl být potenciálně škodlivý?**	**ano**	**45**
		ne	**46**
5.2.	**Setkali jste se již někdy s napadeným médiem (zavirovaný USB flash)?**	**ano**	**44**
		ne	**47**
5.3.	**Setkali jste se u sebe nebo u někoho ve svém okolí se závažnými problémy v souvislosti se selháním techniky (selhání počítače, ztráta dat a jiné)?**	**ano**	**70**
		ne	**21**
5.4.	**Jakým způsobem byl problém řešen?**	**vyřešil jsem sám**	**17**
		využil jsem služeb odborníka	**53**
5.5.	**Jakým způsobem byl problém řešen?**	**vyřešil jsem sám**	**17**
		využil jsem služeb odborníka	**53**
5.6.	**Setkali jste se již někdy s policejním vyšetřováním v oblasti počítačové bezpečnosti (napadení počítače hackrem, nelegální software)?**	**ano**	**4**
		ne	**87**
5.7.	**Setkali jste se s jiným narušením bezpečnosti počítače a dat, než zde bylo uvedeno?**	**ano**	**3**
		ne	**88**

Příloha č. 3

Top 10 Antivirus Protection

#1 Antivirus for Home Computers	**Kaspersky Internet Security 2010**	**Top performance and easy administration**
#1 Business User Antivirus	**Norton Endpoint Protection Small Business Edition**	**Offers instant protection against new threats!**
#1 Centralized Antivirus Solution	**Kaspersky Work Space Security**	**Very easy centralized solution for many workstations**
#1 Servers and Network Antivirus	**Symantec Protection Suite Small Business Edition**	**Very advanced server product also for mail-servers**

There are 10-15 large antivirus brands to choose from and although most seem relatively similar there are a number of significant differences. The most important are price, usability, performance and management. Since there are several different types of uses, we have divided them into four categories and listed the best antivirus in each category.

Our top 10 list is based on a number of tests as well as the reviews and ratings by renowned magazines and websites - links to these can be seen below.
Price is based on the cheapest available version at the cheapest possible online sales channel. Usability is based on user interface and warnings.

Performance is based on the system-slowdown, detection and protection level including penalties for false-alerts. Management is based on options for all sorts of configuration.

For Home Computers

1. Kaspersky Anti-Virus 2010
2. Symantec Norton AntiVirus 2010
3. BitDefender Antivirus 2010
4. Eset NOD32
5. Panda Antivirus Pro 2010
6. Alwil Avast 4 Professional Edition
7. Grisoft AVG 7.5 Professional
8. Trend Micro
9. McAfee VirusScan
10. F-secure

Zdroj: <http://www.top10list.com/top,10,antivirus,protection/top-ten-antivirus-protection.asp>